# Response Process in the Event of a Data Breach

## Summary

This article describes the basic reactive process involved in responding to a known or suspected Data Breach. It is important to note that the Data Breach, ransomware and malware landscape is a volatile and rapidly evolving threat landscape with new variants and threats arising constantly. This means that remediation, restoration and recovery efforts will be highly incident and case specific and may require varying amounts of time and levels of technical skill, depending on the specifics of the incident at hand.

The information provided in this document is of a general nature and is not client or site-specific. For more tailored information and proactive planning specific to your environment, we recommend undertaking more formal Data Breach Response and Business Continuity Planning, where Maxsum will work with you to assess and map the most likely disaster scenarios and undertake training and testing to ensure that goals and plans around recovery and restoration are realistic and appropriate.

## Signs & Symptoms of a Data Breach

Users or employees might suspect or become aware of a Data Breach in any one of a number of ways including, but not limited to:

- Unexpected emails requesting the transfer or movement of money either sent or received by users;
- Users receiving emails from addresses that do not exactly match that of whom they are claiming to be;
- A user may be notified of an attempt to illegitimately access a system or file;
- A user might suddenly report being unable to open files or notice missing files;
- A user might receive a lock out, or ransom message on their screen with ransom demands;
- Monitoring systems may detect or report unauthorised access or an attack/infection;
- Routine scanning by Maxsum may detect suspicious activity or evidence of unauthorised access, or attack/infection.

## Steps Involved in Responding to Data Breach

### 1. Detection & Reporting

If a data breach is detected or suspected, it is vital that you notify your internal Management team and Maxsum immediately.

### 2. Assessing & Containing the Breach

At this stage the priority is to limit communication between impacted systems and to block access malicious actors may have gained to files and systems.

In the early stages of investigating a data breach, typically we encounter two scenarios:

- Malicious actor(s) may be using your credentials for the purpose of launching further phishing attacks;
- Malicious actor(s) may have actively downloaded data and personally identifiable information (PII) for fraudulent use.

Typical actions that might be taken at this stage to halt and remediate a data breach might include, but not be limited to:

- Checking that the network auditing or logging systems are enabled;
- Changing all passwords and locking credentials for all users;
- Checking for and disabling forwarding rules that malicious actors may have installed.

The scope and severity of the breach will determine the type of resolutions that will be required. Other more involved resolutions may involve running antimalware or other detection scans, updating your system, or even restoring data from backups. In certain cases, there may even be a need to implement mobile device management processes if data needs to be wiped from lost or breached devices.

## 3. Identifying the Source of the Data Breach

Sometimes data breaches occur for reasons so unexpected they can be virtually impossible to prepare for or mitigate. More often than not they are the result of purely opportunistic attacks or simple human error, rather than any technical issue.

The most common source of data breaches by far is an end user unwittingly entering their credentials after receiving a phishing email.
Alternative sources may be found to be VPN logins from a public network, system patching vulnerabilities, etc.

Wherever possible the source of the breach should be identified as best as possible to facilitate further end user training and implement steps to prevent breaches of a similar nature from occurring again. However, in some cases, the exact source of the breach may remain unidentifiable.

## 4. Assessing the Damage

Depending on the nature of the data breach experienced, it may be difficult to initially determine the full extent of the data accessed or exported from your systems.

Depending on the breached individuals' role in the organization, the attacker(s) would potentially have had access to data and files that individual has access to. The potential severity and impact of the compromise is dependent on the sensitivity of the data accessible by that individual, whether the individual has access to accounts payable/receivable or payment data, and its value as Personally Identifiable Information (PII). Depending on the extent of data accessible by the individual, and therefore the attacker, there could potentially be sufficient information made available to the attacker(s) to:

- Conduct some basic identity theft actions targeting persons/staff/customers or other parties whose contact details were available in data accessible from the individuals mailbox(es);
- Contact staff, users or customers and pretend to be affiliated with your company and ask for credit card details;
- Initiate business email compromise or other phishing attacks.

The full extent of the information accessed by the attacker is often unknown at this stage.

## 5. Reporting on Possible Outcomes

Once all the information has been gathered, Maxsum will contact you with an assessment of the likely outcomes and offer a very rough estimate of how long recovery/restoration might take, if required. During this time Maxsum technicians will be in regular contact with your designated contact to execute remedial actions and ensure systems are secure and safe to reuse.

Once the initial remediation is complete and any immediate threat is eliminated, Maxsum will provide a summary of the remediation efforts, known facts up to that point, and recommendations for next steps. This will be provided in the form on a report titled ***Preliminary Data Breach Investigation Findings***.

## 6. Determining if the Data Breach is a "Notifiable Data Breach"

As Maxsum technicians provide you with ongoing updates and once you are provided with the *Preliminary Data Breach Investigation Findings*, you will need to hold some internal discussions and seek legal or other advice as soon as possible to determine:

- If communicating details of the breach to affected parts is warranted;
- If the breach has triggered Reporting Obligations under the Notifiable Data Breaches Scheme or other regulations
  ***Note:*** *As of February 2018, Australian organisations are subject to mandatory data breach notification requirements under Australia's Privacy Act (Cth). More details on this can be found at:*

  - www.maxsum.com/blog/data-breach-response-planning-101
  - www.oaic.gov.au

Based on preliminary investigation into a cyber incident conducted by Maxsum and provided to you, it may prudent for you to seek independent legal advice to determine whether the incident can be classified as an "eligible data breach" under Australia's Notifiable Data Breaches Scheme, and therefore require notification to the Office of the Australian Information Commissioner (www.oaic.gov.au). However, as eligible data breaches must be notified to the OAIC within 30 days of discovery, it would be our recommendation that, legal advice be sought as soon as practicable.

Communicating with affected parties may involve sending email notification and advice to affected parties or providing public notification of the breach via your website or other channels. In any case, you will need to work with your Human Resources, Public Relations or Legal advisors to ensure that communications cover:

- The nature of the breach
- The remedial actions that have been taken
- Any foreseeable risk to affected parties
- Advice to affected parties
- Steps the organisation is taking to prevent similar incidents from occurring in the future.

## 7. Further Recommendations

Based on Maxsum's general and specific advice provided in the ***Preliminary Data Breach Investigation Findings*** report, there may be some technical upgrades or implementations, communications or training recommendations that require actioning to prevent similar breaches from occurring in the future.

Our recommendations following on from the preliminary investigation stage might typically include, but not be limited to, advice to organisations:

- To email all recipients of the malicious/spam email:
  - providing an explanation and advice not to open suspicious links, attachments or communications, and
  - prompting them to reset their password as a security measure.
- To remind staff to remain vigilant around Phishing and password disclosure, including:
  - an explanation and advice not to open suspicious links, attachments or communications, and
  - prompting them to reset their password as soon as possible and regularly thereafter, as a security measure.
- To conduct staff training on password security.
- To enable multifactor authentication to assist in prevent future breaches of a similar nature.

## 8. Review and Training

Once remediation and restoration efforts are complete, Maxsum will work with your executive team, at your request, to review the incident with a view to improving systems and processes to assist in preventing compromises of a similar nature in future. This might involve technology, business process, or staff training audits, reviews and planning.

**Disclaimer:** *The information provided by Maxsum does not constitute legal advice. The information provided by Maxsum is the result of our investigative processes prompted in response to a client or partner's discovery of the incident, and is based on Maxsum's subsequent investigation of the incident conducted to the extent possible through our channels and our general knowledge on the theoretical and potential usage of hacked or breached personal information. Organisations must seek their own legal advice with regard to their compliance requirements under the Notifiable Data Breaches Scheme and use the information provided by Maxsum only as part of their own Data Breach Response investigative process.*

# Process Summary and Overview

A graphic representation of the process described in this document with accompanying reporting lines and actions is provided as an Appendix to this document on Page 5.

# More Information

More information on data breach prevention and remediation is available at www.maxsum.com/blog and www.oaic.gov.au.

Contact Maxsum on **1300 629 786** to discuss your data breach prevention and remediation processes.

# Client Data Breach Response Process